

## **REMARKS**

In view of the preceding amendments and the following comments, and pursuant to 37 C.F.R. § 1.111, Applicant respectfully requests reconsideration of the Office Action.

### **Summary of the Amendment**

Applicant has amended claims 48-64. Support for the amendments can be found in the originally filed claims and the Application, at least at ¶¶ 0043, 0048, 0053, 0057, 0087, 0100, 0112, 0134, and 0136-0137, and Figures 1, 2, and 10. The amendments do not add new matter. The Applicant respectfully requests reconsideration of pending claims 48-64, and allowance of the present application in view of the amendments and the following remarks.

### **Detailed Remarks**

#### **I. Statutory Subject Matter under 35 U.S.C. § 101**

The Office Action rejected claims 49, 51, 61 and 64, under 35 U.S.C. § 101 as directed to non-statutory subject matter. The Office Action, at pages 3-4, asserts that claims 49, 51, 61 and 64 are "directed to non-statutory subject matter as failing to fall within a statutory category of invention." The Applicant respectfully traverses these rejections.

#### **Claims 51 and 64**

Claim 51, as amended, recites a computer program recorded therein, when executed by a processor, stores in a memory and enrolls, by a transmitter sub-system, biometric signatures into a database of biometric signatures. Claim 51 also recites a system comprising a processor, the memory, the transmitter sub-system and a receiver sub-system. Claim 51 further recites code, when executed by the processor, that stores a biometric signal received by the transmitter sub-system in the memory and database; and code, when executed by the processor, that enables administrative processing of information stored in the memory and database.

Applicant submits *In re Bilski* established that a claimed process is directed to statutory subject matter, under 35 U.S.C. § 101, where the process is tied to a particular machine or apparatus, or the process transforms a particular article into a different state or thing. (See *In re Bilski*, 88 USPQ2d 1385, 1391 (Fed. Cir. 2008)). Consistent with the *Bilski* decision, MPEP 2106, at page 2100-11, recites the same test. Claim 51 defines a machine comprising a processor, a memory, a database, and code executed by the processor that stores a biometric signal and enables administrative processing of information stored in the memory and database. 35 U.S.C. § 101 permits machines to be patented. Thus, claim 51 recites statutory subject matter.

Claim 64, as amended, recites a computer program recorded therein, when executed by a processor, executes a method to enroll, by a transmitter sub-system, biometric signatures into a memory and a database of biometric signatures. Claim 64 also recites system comprising (a) said memory and said database. Claim 64 further recites code, when executed by the processor, that receives and stores a biometric signal, classifies a legitimate sequence of one or more biometric signal, and performs at least one of (a) amending information stored in the database, and (b) classifying a subsequent biometric signal. For at least the reasons noted therefore, claim 51, as amended, claim 64 recites statutory subject matter.

#### Claims 49 and 61

The Office Action, at page 4, asserts that claims 49 and 61 comprise a series of "logic" directed towards functional descriptive material. The Applicant respectfully traverses these rejections.

Claim 49, as amended, recites system further including a processor, a memory, and a receiver sub-system. Claim 49 also recites means for enrolling biometric signatures into the memory and a database. The Applicant respectfully submits that Fig. 1 clearly shows that the transmitter sub-system 116 comprises structural elements including a code entry module 103 (which includes an audio transducer 124, an LED indicator 122, and a bio sensor 121), a controller transmitter

107, and a database 113. The Application, at ¶ 0087, discloses a user ID database 105 may also form part of the transmitter sub-system 116 or alternately this database 105 may be incorporated into the receiver sub-system 117. The Application, at ¶ 0134, discloses functional interworking of the aforementioned structural elements can, in one example, be provided by processors 107 and/or 109 executing the appropriate software. The Application, at ¶ 0109, discloses the term "enroll" refers to the administration function for loading relevant signatures into a database. Considering the *means for enrolling biometric signatures into a database*, as described in the Application, at ¶¶ 0104 and 0123, if the used ID database 105 is empty, a biometric signal received by the biometric sensor 121 is stored in the user database 105 as a first administrator. Clearly, therefore, the *means for enrolling* should be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof (35 USC 112(6)), being at least the biometric sensor 121, the transmitter 107, as well as processors 107 and 109 (see Application at ¶ 0134), and equivalents thereof. Thus, the features of claim 49 are not directed to software per se, and accordingly, claim 49 recites statutory subject matter, under 35 U.S.C. § 101.

Claim 49 further recites means for providing the accessibility attribute when a legitimate biometric signal is received. The Application, at ¶ 0079, discloses when a request 102 (for example, a thumb press on the biometric sensor panel 121) is authenticated by the code entry module 103 against biometric signatures for authorized users in the user database 105, then the code entry module 103 sends a signal 106 to a controller/transmitter 107 which sends an access signal 108 to a controller 109 in the receiver sub-system 117 which in turn sends a command 110 giving access to a controlled item 111.

The authentication of the biometric signature matching produces an accessibility attribute for the biometric signal 102 in question (see the Application at ¶ 0093). Clearly, therefore, the *means for providing the accessibility attribute* should be construed to cover the corresponding structure, material, or acts described in the

specification and equivalents thereof (35 USC 112(6)), being at least the biometric sensor 121, the transmitter 107, as well as processors 107 and 109 and the associated software, and equivalents thereof. Thus, *means for providing the accessibility attribute* is not directed to software per se, and accordingly is statutory.

The Applicant respectfully submits that, for at least the reasons noted above, claim 49 recites statutory subject matter, under 35 U.S.C. § 101.

Claim 61 recites similar features to those referred to above in regard to claim 49. Thus, for at least the reasons noted above, claim 61, as amended, recites statutory subject matter, under 35 U.S.C. § 101.

## **II. Rejections Under 35 U.S.C. § 103**

The Office Action rejected claims 48, 49, 52, and 61, under 35 U.S.C. § 103(a) as unpatentable over Martin et al. (WO 01/71462) in view of Hoffman et al. (U.S. Patent No. 7,152,045). The Office Action rejected claims 62-64, under 35 USC 103(a) as unpatentable over Hoffman in view of Martin and further in view of Koo et al. (WO 02/12660). The Office Action rejected claims 50-51 and 53-60, under 35 U.S.C. § 103(a) as unpatentable over Hoffman in view of Koo.

### **Claims 48, 49, 52 and 61**

Independent claim 48 as amended recites, among other features, *a transmitter subsystem for enrolling biometric signatures into a database, using a legitimate sequence of one or more biometric signals to enroll each biometric signature, and for providing an accessibility attribute when a legitimate biometric signal is received*. The Application, at ¶ 0109, provides support for these recited features. According to the Application the “sequence of one or more biometric signals” can be understood, according to one described example, by “a succession of finger presses to the biometric sensor 121”. The term “legitimate sequence” can be understood, according to one described example, by meeting criteria that “these successive presses are of the appropriate duration, the appropriate quantity, and are

input within a predetermined time". The Office Action, at page 5, asserts that Martin, in combination with Hoffman, teaches or suggests all the features of claim 48.

However, Martin, even in combination with Hoffman, does not teach, suggest or disclose all the features of claim 48. Instead, Martin is directed to a system and method for secure biometric identification (Abstract). Martin is concerned with authenticating the identity of a user in order to enable the user to access electronic devices and systems (page 1 lines 27-30). Martin describes an arrangement having a mobile device and a server (page lines 21-22). In one example of Martin (page 3 line 23) the mobile device is a Personal Digital Assistant (PDA) incorporating, in an expansion slot, a card having a fingerprint sensor (page 4 lines 1-10). When a user of the PDA wishes to access a secure device (which in the example is an encrypted database 34 on the PDA itself – see Fig. 2 and page 4 lines 28-29) the user places a finger on the fingerprint sensor 28 on the PDA which sends an encrypted version of the scanned fingerprint to the server 40 (page 6 line 29 – page 7 line 3). The server 40 decrypts the signal and compares the decrypted fingerprint against a database of authorised fingerprints 54 (which is on the server – see Fig. 3) to determine if the request is valid (page 7 lines 11-16). If the request is valid the server retrieves a decryption key for the secure device 34 (see page 7 lines 17-19) and sends it back to the mobile device which is then able to access the secure database 34 (see page 7 lines 20-29). The Office Action, at page 5, asserts that Martin teaches *a transmitter subsystem for enrolling ... biometric signatures into a database*. However, Martin appears to be silent about *enrolment* and makes no mention of how the authorized fingerprints are loaded into the database 54 of Martin. The database 54 of Martin is only referred to twice in the citation, at page 5 line 18 and page 7 line 16. Nowhere does Martin teach, suggest, or disclose a method for enrolling fingerprints into the database 54, and nowhere does Martin use of the term "enrol" or any similar term. Accordingly, Martin does not teach, suggest, or disclose *enrolling ... biometric signatures into a database*, as claimed.

The Office Action, at page 5, concedes that Martin is silent in regard to the *accessibility attribute* and refers to Hoffman in this regard. However, Hoffman fails to fill the gap left by Martin. Instead, Hoffman is directed to a token-less identification system and method for authorization of transactions and transmissions (Abstract). A "token" in this citation is an inanimate object such as a plastic card which confers a capability to the individual presenting the object (column 1 lines 25-29). The citation compares a biometric sample such as a finger print, gathered directly from the person of an unknown user, with an authenticated biometric sample of the same type obtained and stored previously (Abstract). Fig. 1 of Hoffman shows the overall configuration of the described arrangement. A Data Processing Centre DPC 1 is connected to terminals 2 through various communication means 3 (column 12 lines 52-54). The citation refers to a number of different terminals (column 27 line 21 – column 28 line 7). Each terminal is associated with a Biometric Input Apparatus (BIA) which is a combination of hardware and software whose job is to gather, encode, and encrypt biometric input for use in individual identification (column 14 lines 38-45).

As previously noted, claim 48 as amended recites, among other features, *enrolling biometric signatures into a database, using a legitimate sequence of one or more biometric signals to enroll each biometric signature.*

Registration is performed in Hoffman using a Biometric Registration Terminal (BRT) (column 27 lines 25-29). The purpose of the BRT (column 36 lines 44-50) is to register new individuals including their biometric-PIC (Personal Identification Code – see column 2 line 9), mailing address, private code, electronic mail addresses, a list of titles and title index codes used to send and receive electronic messages and faxes, and a list of financial asset accounts and account index codes that they can access, all using their biometric-PIC. Clearly this amount of data entry requires, as well as a biometric sensor for inputting the biometric-PIC, a standard keyboard for entering the data. In contrast, claim 48, as amended, recites enrolling *using a legitimate sequence of one or more biometric signals to enroll each biometric*

*signature* (see Application at ¶ 0109) rather than using keystrokes applied to a standard terminal. This approach of enrolling *using a legitimate sequence of one or more biometric signals* considerably simplifies the implementation of the user interface, since the *one or more biometric signals* are clearly provided via the biometric sensor alone. Hoffman is not concerned with simplifying the user interface for the enrolment process, and accordingly clearly uses a standard keyboard for data entry, in clear contrast to claim 48.

Claim 48 as amended recites, among other features, *a (single) transmitter subsystem* (emphasis added) *for enrolling biometric signatures into a database ... and for providing an accessibility attribute when a legitimate biometric signal is received*. In other words the same device (*transmitter sub-system*) in claim 48 as amended performs both the enrolment and the access signal provision functions.

In contrast to claim 48, while Hoffman does describe a registration process (Fig. 10), the citation appears to limit performance of the registration process to Biometric Registration Terminals (BRT) (column 36 lines 42–55). Since BRTs are located in places that are physically secure such as retail banking outlets (column 36 line 66 – column 37 line 3) and no similar limitation appears to be placed on the other terminals, it seems clear that of all the terminals described in Hoffman, only the BRT performs an enrolment function, while the other terminals appear only able to access controlled items. Accordingly, Hoffman does not disclose *a (single) transmitter subsystem for (a) enrolling biometric signatures into a database ... and for (b) providing an accessibility attribute when a legitimate biometric signal is received*. In fact, the separation of functions and the need for a secure environment for the BRTs teaches away from terminals performing both features (a) and (b) as in claim 49 as amended. Moreover, Hoffman does not teach, suggest, or disclose the following features:

- *enrolling biometric signatures into a database, using a legitimate sequence of one or more biometric signals to enroll each biometric signature; OR*

- *a transmitter subsystem for enrolling biometric signatures into a database ... and for providing an accessibility attribute when a legitimate biometric signal is received*

Establishment of a prima facie case of obviousness requires that the prior art references when combined must teach or suggest all the claim limitations. However, Hoffman, even in combination with Martin, does not teach, suggest, or disclose *a transmitter subsystem for enrolling biometric signatures into a database, using a legitimate sequence of one or more biometric signals to enroll each biometric signature, and for providing an accessibility attribute when a legitimate biometric signal is received.*

For at least the reasons noted therefore, it is submitted that claim 48 as amended is patentable over the cited references, taken alone or in combination.

Claims 49, 52 and 61 have been amended to recite similar features to those referred to above in regard to claim 48 as amended. For at least the reasons noted therefore, claims 49, 52, and 61, as amended, are patentable over the cited references, taken alone or in combination.

#### **Claims 62-64**

Claim 62, as amended, recites *means for, when an administrator signature has been stored in the database, classifying a legitimate sequence of one or more biometric signals, each signal matching the administrator signature, as control information; and means for performing at least one of (a) amending information stored in the database depending upon the control information, and (b) classifying a subsequent biometric signal as one of an administrator signature and an ordinary signature depending upon the control information.* The Office Action, at page 11, asserts that Hoffman, in combination with Martin and Koo, teaches or suggests all the features of claim 62.

However, Hoffman, even in combination with Martin and Koo, does not teach, suggest or disclose all the features of claim 62. The Office Action, at pages 11-12, concedes that the combination of Hoffman and Martin is silent in regard to the



features recited in claim 62, and refers to Koo in this regard. However, Koo fails to fill the gap left by Hoffman and Martin. Instead, Koo is directed to door lock arrangements using portable fingerprint recognition keys (page 1 lines 6-8). One of the objects of Koo is to provide an electronic card key which is capable of registering fingerprint (s) of one or more users, authenticating the users utilizing the fingerprints information, locking/unlocking one or more doors, and storing access information of the user (s) (page 4 lines 6-9). As a precursor to registering a user's fingerprint on a key card according to Koo, one or more administrator's fingerprints are registered according to the process depicted in Fig. 6 as described at page 16 lines 3 – 25. Once at least one administrator has registered fingerprints on the card key, the user to be registered "receives the key card (from the administrator) and the user selects the user registration menu of the card key (page 17 lines 14-15). Then, the user enters their fingerprint code (page 17 lines 22-23) without any participation of the administrator. Nowhere does Koo teach, suggest, or disclose that the registered administrator must input *a legitimate sequence of one or more biometric signals ... as control information* (emphasis added) to enable the user to register. The *control information* according to claim 62, as amended, is a distinct element to the *administrator signature* that has been stored in the database, and is used as a precursor to enabling registration of a user. Nowhere does Koo teach, suggest, or disclose *legitimate sequence of one or more biometric signals, each signal matching the administrator signature, as control information*. Koo uses a quite different approach than recited by claim 62, as noted above.

Establishment of a prima facie case of obviousness requires that the prior art references when combined must teach or suggest all the claim limitations. However, Hoffman, even in combination with Martin and Koo, does not teach, suggest, or disclose *means for, when an administrator signature has been stored in the database, classifying a legitimate sequence of one or more biometric signals, each signal matching the administrator signature, as control information; and means for performing at least one of (a) amending information stored in the database*

*depending upon the control information, and (b) classifying a subsequent biometric signal as one of an administrator signature and an ordinary signature depending upon the control information.*

For at least the reasons noted therefore, claim 62, as amended, is patentable over the cited references, taken alone or in combination.

Claims 63 and 64 have been amended to recite similar features to those referred to above in regard to claim 62 as amended. For at least the reasons noted therefore, claims 62-64, as amended, are patentable over the cited references, taken alone or in combination.

**Claims 50-51 and 53-60**

Claim 50, as amended, recites *enabling administrative processing of information stored in the database when a legitimate sequence of biometric signals, each signal matching the stored administrator signature, is received by the transmitter*. The Office Action, at page 15, asserts that Hoffman, in combination with Koo, teaches or suggests all the features of claim 50.

However, Hoffman, even in combination with Koo, does not teach, suggest or disclose all the features of claim 50. As previously noted above, Hoffman performs registration using a Biometric Registration Terminal (BRT) having a standard keyboard. Hoffman is not concerned with simplifying the user interface for the enrolment process, and does not teach, suggest, or disclose use of *a legitimate sequence of biometric signals, each signal matching the stored administrator signature*. A similar submission applies to Koo as noted above.

Establishment of a prima facie case of obviousness requires that the prior art references when combined must teach or suggest all the claim limitations. However, Hoffman, even in combination with Koo, does not teach, suggest, or disclose *enabling administrative processing of information stored in the database when a legitimate sequence of biometric signals, each signal matching the stored administrator signature, is received by the transmitter*.

For at least the reasons noted therefore, claim 50, as amended, is patentable over the cited references, taken alone or in combination.

Claims 51 and 53-60 recite similar features to those referred to above in regard to claim 50 as amended, either directly or by dependency. For at least the reasons noted therefore, claims 51 and 53-60, as amended, are patentable over the cited references, taken alone or in combination.

### **Conclusion**

In view of the above amendments and remarks, Applicant respectfully submits that this application is in condition for allowance and such action is earnestly requested. If for any reason the Application is not allowable, the Examiner is requested to contact the Applicant's undersigned attorney.

Respectfully submitted,

BRINKS
HOFFER
GILSON
& LIONE



Robert D. Summers Jr.  
Registration No. 57,844  
Attorney for Applicant

BRINKS HOFER GILSON & LIONE

**CUSTOMER NO. 00757**

Telephone: (312) 321-4200

Facsimile: (312) 321-4299